

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case No.24-935M(NJ)  
The residence, vehicle, and person of )  
Michael G. CEMAN )  
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Wisconsin  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/20/2024 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

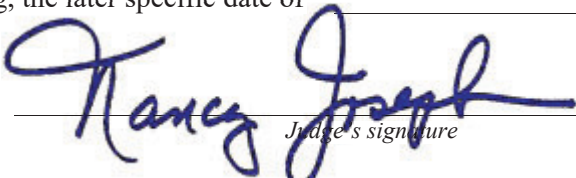
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)  
☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:12/6/2024 @ 4:17 p.m.

City and state: Milwaukee, Wisconsin

  
Judge's signature

Nancy Joseph, U.S. Magistrate Judge

Printed name and title

## Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

---

*Executing officer's signature*

---

Printed name and title

## ATTACHMENT A

### *Property/person to be searched*

1. The PREMISES located at N2607 County Road Q, Markesan, Wisconsin 53946, further described as single-family, two-story home with an attached two car garage, brown siding and brown shingles. The premises sits on approximately 41 acres of property, which also includes four outbuildings/sheds/storage buildings. One of the buildings is a wooden outbuilding. There is a large wooden barn and a large storage building with light gray siding and black shingles. Lastly, there is a large blue shed located on the property.



The PREMISES (residence)



The PREMISES (outbuilding)



The PREMISES (barn and storage building)



The PREMISES (barn, building, and shed)

2. CEMAN's VEHICLE, further described as a red 2011 Chevrolet Silverado, bearing Wisconsin Registration GJ6336, and having VIN 3GCPKSE34BG339494.
3. The person of Michael G. CEMAN (Male/White, DOB 07/01/1957).

## **ATTACHMENT B**

### *Property to be seized*

Evidence of violations of 18 U.S.C. §§ 922(a)(1) (dealing firearms without a license) and 18 U.S.C. §§ 933 (firearms trafficking) involving, Michael G. CEMAN (Male/White, DOB 07/01/1957), including the following relating to such offenses:

- a. Records showing CEMAN's identity and any persons who supplied and acquired firearms to/from CEMAN;
- b. Records of purchases, transfers, and sales of firearms;
- c. Records of CEMAN's schedule, travel, and location at relevant times;
- d. CEMAN's financial records, such as bank accounts/statements, checks, and credit card bills;
- e. Relevant pictures, videos, IP addresses, contact information, and contact lists;
- f. Text messages, social media messages and content, SMS messages, iMessages, and related data regarding the sale and trade of firearms and controlled substances;
- g. E-mail content and addresses relating to the sale and trade of firearms and controlled substances;
- h. Computers or storage media used as a means to commit or facilitate the violations described above, including mobile/cellular phones;

For any computer or storage media that is authorized to be seized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise covered by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including



firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

The terms “records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.



## UNITED STATES DISTRICT COURT

for the  
Eastern District of WisconsinIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The residence, vehicle, and person of  
Michael G. CEMAN

Case No. 24-935M(NJ)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ Wisconsin \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 922(a)(1)	Dealing firearms without a license
18 USC 933	Firearms trafficking

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BRADLEY KURTZWEIL

Digitally signed by BRADLEY KURTZWEIL  
Date: 2024.12.05 15:28:53 -06'00'

Applicant's signature

Bradley Kurtzweil, ATF Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
 \_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 12/6/2024

City and state: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**  
**UNDER RULE 41**

I, Bradley Kurtzweil, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises described in Attachment A and occupied by Michael G. CEMAN (Male/White, DOB 07/01/1957) known as N2607 County Road Q, Markesan, WI 53946, hereinafter “PREMISES,” a 2011 Chevrolet Silverado, bearing Wisconsin Registration GJ6336, and having VIN 3GCPKSE34BG339494, hereinafter, “VEHICLE,” for the property described in Attachment B.

2. I am a Special Agent of the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since March 2020. My duties with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I completed approximately 26 weeks of training (approximately 1000 hours) at the Federal Law Enforcement Training Center (Glynco, Georgia) and ATF’s National Academy. The training included courses on constitutional law such as search and seizure, and conducting investigations through searches, arrests, interviews, surveillance, and evidence collection.

4. During my time at ATF, I have attended specialized training from the ATF related to the determining the interstate NEXUS of firearms and ammunitions. I regularly perform physical examinations of firearms for various purposes, including a determination of interstate/foreign commerce nexus and appropriate classification under the Gun Control Act of 1968. Additionally, I frequently conduct research by referencing industry-related public reference materials widely utilized by law enforcement and civilian firearms experts, manufacturer’s websites, law

enforcement reports, records maintained by ATF as part of its function to regulate the firearms and ammunition industry, as well as conversations with manufacturers and/or other experts in the industry. I have also interviewed multiple individuals involved in firearms and drug trafficking, obtaining information regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances, resulting in prosecutions, convictions and the seizure of illegal drugs and weapons.

5. Prior to joining ATF, I was a sworn Police Officer in the State of Illinois from March 2011 to March 2020. I completed 12 Weeks (approximately 480 hours) of basic training at the Illinois State Police Academy from April 2011 to June 2011.

6. My most recent position was with the Bolingbrook Police Department in Bolingbrook, Illinois, where I was a Patrol Officer from December 2012 until March 2020. From July 2017 until March 2020, I also served as an Evidence Technician, assigned to Patrol.

7. During my career as a Police Officer, I attended approximately 520 hours of additional training in areas including evidence collection, interview/interrogation, arson and explosives, gang investigations, and drug investigations.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 922(a)(1) (dealing firearms without a license) and 18 U.S.C. §§ 933 (firearms trafficking) have been committed, are being committed, and will be committed by Michael G. CEMAN (Male/White, DOB 07/01/1957), of Markesan, WI. There is also probable cause to search CEMAN, the PREMISES and the VEHICLE described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

### **PROBABLE CAUSE**

10. In September 2014, ATF Milwaukee Industry Operations (IO) received a referral from the State of Wisconsin Department of Justice (WDOJ) Crime Information Bureau regarding information they had received about Federal Firearms Licensee (FFL) John L. Lauritzen, operating as Lauritzen Enterprises, regarding purchases made by Michael G. CEMAN. The referral advised that CEMAN appeared to be structuring handgun purchases in a manner to avoid multiple sales reporting on ATF Form 3310.4 – Report of Multiple Sale or Disposition of Pistols or Revolvers (“Report of Multiple Sale”), and that CEMAN had asked Lauritzen to submit separate background checks to the WDOJ Firearms Unit for each individual handgun that CEMAN purchased, even when purchasing more than one handgun on the same occasion. CEMAN reportedly believed that if individual handguns were purchased with separate background checks, even when purchased at the same time, then a Report of Multiple Sale need not be submitted to ATF. The referral also stated Lauritzen did not understand that multiple handgun sales must be reported if transfers occurred to the same purchaser within five-business days. Due to this apparent reporting noncompliance, Industry Operations Investigator (IOI) Miguel Ruiz initiated a compliance inspection of Lauritzen Enterprises on December 1, 2014, resulting in citations for violations, which included failure to submit multiple handgun sales reports. Lauritzen later advised IOI Ruiz that he had told CEMAN of the violations found during the ATF inspection and explained the multiple reporting rules to CEMAN at that time.

11. In May 2016, IOI Ruiz identified and reviewed firearms purchases made by CEMAN from March 2015 to May 2016 and determined CEMAN appeared to be structuring purchases at several different FFLs to avoid the multiple-sales reporting requirement. As a result, on May 16, 2016, IOI Ruiz sent a referral (2016-0016) to the ATF Milwaukee Criminal Enforcement (CE) division for follow up into CEMAN’s firearms purchases.

12. On May 26, 2016, ATF Special Agent (retired) Sandra DeValkenaere opened ATF Case 778040-16-0058 into possible violations of Federal firearms laws by CEMAN. At the time SA DeValkenaere opened her investigation, she determined CEMAN conducted 15 purchases of multiple firearms, including purchasing more than one handgun or revolver within a 5-day period from the same FFL. SA DeValkenaere also determined that law enforcement recovered 3 firearms, traced to CEMAN, during firearms-related offenses. Specifically, those recoveries were by US Customs in Virginia – 761-day Time to Crime (TTC); the Brown County Sheriff's Office in Green Bay, WI – 356-day TTC; and the Milwaukee Police Department in Milwaukee, WI – 321-day TTC. Time to Crime is the amount of time from when the firearm is originally purchased to when it is recovered by law enforcement. SA DeValkenaere also determined that CEMAN had purchased firearms from at least 10 different FFLs.

13. On June 6, 2016, SA DeValkenaere and a Green Lake County Sheriff's Office Deputy met with CEMAN at his residence. At that time, CEMAN stated he kept no records of his firearms purchases or sales. He also admitted that he frequented gun shows, where he shared a table with a friend. At this time, SA DeValkenaere advised CEMAN of federal law pertaining to the selling of firearms and served CEMAN with an ATF Warning Notice of Unlicensed Dealing of Firearms in Violation of Federal Law, which CEMAN signed. Believing CEMAN would not continue the same purchasing and selling behavior, SA DeValkenaere subsequently closed her investigation into CEMAN.

14. In February 2017, SA DeValkenaere renewed her investigation into CEMAN when she learned he continued to purchase firearms after June 6, 2016. Efforts to surveil CEMAN in November and December 2017 were unsuccessful at locating him at local gun shows where he was believed to be reselling the firearms that he had purchased. In February 2018, the investigation into CEMAN was again closed due to SA DeValkenaere's impending retirement.

15. In December 2023, IOI Ruiz conducted a compliance inspection at FFL Wildo Corp., d/b/a Holliday Food & Sport, in Waupun, WI covering December 12, 2022, to December 12, 2023. IOI Ruiz determined that during this one-year timeframe, CEMAN had purchased 101 firearms from FFL Wildo Corp., d/b/a Holliday Food & Sport, in Waupun, WI. IOI Ruiz also determined that CEMAN had made additional firearms purchases from this FFL prior to the December 12, 2022, to December 12, 2023, timeframe. Regarding these firearms purchases, IOI Ruiz observed that CEMAN still appeared to be structuring his purchases to avoid multiple sales reporting laws. On March 4, 2024, another referral was sent by IOI Ruiz to the ATF Milwaukee CE division for investigation into CEMAN's purchasing and selling habits (LEAD 24-1117). The case was assigned to your Affiant.

16. Your Affiant identified 12 instances between June 2015 and August 2024 when firearms, originally purchased by CEMAN, were recovered during firearms-related offenses. Your Affiant noted that 8 recoveries were of firearms that CEMAN purchased after SA DeValkenaere had served him with the ATF warning notice. Your Affiant observed the TTCs of the 12 recoveries ranged from 259 days to 1596 days, with recoveries by Customs and Border Protection (CBP) in Norfolk, VA (1 firearm); Brown County Sheriff's Office in Green Bay WI (1 firearm); Milwaukee Police Department in Milwaukee, WI (3 firearms); Drug Enforcement Agency (DEA) in Milwaukee, WI (1 firearm); Brooklyn Park Police Department in Brooklyn Park, MN (1 firearm); Clark County Sheriff's Office in Vancouver, WA (1 firearm); Waukegan Police Department in Waukegan, IL (1 firearm); Madison Police Department in Madison, WI (2 firearms); and St Francis Police Department in St. Francis, WI (1 firearm). Your Affiant determined that between May 8, 2024, and December 5, 2024, CEMAN purchased or attempted to purchase at least 77 firearms from 6 different FFLs, with 26 firearms being purchased or attempted to be purchased since October 1, 2024. Given the numerous firearms purchased by CEMAN and his history of unlicensed firearms

sales, your Affiant believes CEMAN has been building a firearms inventory to again engage in the unlicensed sale of firearms.

17. Your Affiant contacted the Wisconsin DOJ Firearms Unit in May 2024, whose records indicated that CEMAN's phone number was 920-539-9279. Using law enforcement databases, your Affiant determined the Service Provider for 920-539-9279 was Cellco Partnership, d/b/a Verizon Wireless.

18. Your Affiant reviewed Verizon Wireless records, which indicated 920-539-9279 was registered to "Karla Ceman," who resides at N2607 County Road Q, Markesan, WI 53946, which is Michael CEMAN's address per the Wisconsin Department of Transportation (DOT), as well as, the personal address CEMAN recorded on all ATF Forms 4473 (Firearms Transaction record) he completed during firearms purchases at FFL Wildo Corp., d/b/a Holliday Food & Sport, in Waupun, WI from December 12, 2022 to December 12, 2023. On September 23, 2024, your Affiant conducted surveillance of CEMAN at his listed residence, i.e., N2607 County Road Q, Markesan, WI 53946. At approximately, 10:50 a.m., your Affiant observed CEMAN walking in the front yard of this residence and then enter the residence via the front door. A review of the Verizon call history for 920-539-9279 identified approximately seven separate FFLs, six of which are in the Eastern District of Wisconsin, that were contacted by the user of 920-539-9279 between April 4, 2023, and March 3, 2024. On July 28, 2024, CEMAN listed his phone number as 920-539-9279 on a Wisconsin DOJ Firearms Dealer Notification (Handgun Transfers) Form, during the purchase of a firearm at FFL Dunham's Sports in Beaver Dam, WI. Based on the foregoing, your Affiant believes that CEMAN is the current user of 920-539-9279.

19. On August 30, 2024, a federal search warrant (24-M-486) was issued in the Eastern District of Wisconsin and executed on Verizon Wireless for historical cell site records and other phone records pertaining to 920-539-9279. On September 19, 2024, your Affiant received the



requested records from Verizon Wireless and reviewed them. Your Affiant determined that between August 1, 2023, and August 30, 2024, the device assigned call number 920-539-9279 utilized cell towers in approximately the same areas where, and during the same dates and times when, a gun show was being held within the State of Wisconsin. Specifically, the device assigned call number 920-539-9279 was in the vicinity of 13 distinct gun shows on 16 different occasions during this timeframe. One of those gun shows is the Central Wisconsin Gun Collectors Show. According to an event description located at “fdl.com,” which is a website run by “Destination Lake Winnebago Region,” the Central Wisconsin Gun Collectors Show is “The largest gun show in Wisconsin,” which is held three times a year in, “January, April and October.” Based on a historical internet review, this gun show was previously hosted at the Fond du Lac County Fairgrounds on October 21 through October 22, 2023, and January 20 through January 21, 2024. The device assigned call number 920-539-9279 utilized cell towers in Fond du Lac on October 21, 2023, and January 20, 2024. The next Central Wisconsin Gun Collector’s Show was scheduled to occur at the Fond du Lac County Fairgrounds on October 19 and 20, 2024. Based on evidence that CEMAN attended two previous Central Wisconsin Gun Collectors Shows, your Affiant anticipated CEMAN would attend the Central Wisconsin Gun Collectors Show on October 19 and 20, 2024, where he would have the opportunity to sell any number of firearms that he had recently acquired.

20. Based on training and experience, your Affiant knows that in contemporary society people ordinarily keep their electronic devices either near or on their person. Accordingly, your Affiant sought a warrant to obtain location data for the device assigned call number 920-539-9279 to augment investigators’ surveillance of CEMAN. On October 17, 2024, a federal search warrant (24-MJ-216) was issued in the Eastern District of Wisconsin and executed on Verizon Wireless for real time location (phone ping) data pertaining to the device assigned call number 920-539-9279 (the “DEVICE”). On October 19, 2024, location data for the DEVICE indicated the DEVICE was

traveling from CEMAN's home to the Fond du Lac County Fairgrounds, in Fond du Lac Wisconsin, where the Central Wisconsin Gun Show was being held. Based on this information, investigators responded to the Fond du Lac County Fairgrounds.

21. At approximately 09:14 a.m., an investigator observed CEMAN arrive at the Expo Center at the Fond du Lac County Fairgrounds in a red 2011 Chevrolet Silverado Pickup truck, bearing Wisconsin Registration GJ6336 (the "VEHICLE"). CEMAN was the driver of the VEHICLE. According to Wisconsin Department of Transportation records, CEMAN is the registered owner of the VEHICLE. The investigator observed CEMAN park the VEHICLE in the parking lot of the Expo Center at the Fond du Lac County Fairgrounds. CEMAN exited the VEHICLE and walked toward the Expo Center with a handgun case under one arm and carrying an orange cloth bag that contained square boxes. Based on the observing investigator's training and experience, those boxes were consistent with the size and appearance of handgun boxes/cases.

22. At approximately 10:30 a.m., investigators entered the Expo Center and observed CEMAN sitting at the end of a table where multiple firearms were displayed for sale. Investigators could not determine if any of the displayed firearms belonged to CEMAN. However, investigators noted that CEMAN's orange cloth bag, which was laying by his feet, contained no handgun cases/boxes. Several unknown males were seated at the table with CEMAN. CEMAN eventually went to another exhibitor's table where he obtained what appeared to be an ammunition can. Ammunition cans are made of metal or plastic and are used to store loose ammunition rounds or boxes of ammunition. CEMAN returned to his table and placed the ammunition can inside his orange cloth bag. At approximately 11:42 a.m., CEMAN left the Expo Center without the firearms he appeared to have when he first arrived at the gun show and was seen entering his VEHICLE and driving out of the Expo Center parking lot. He did not return to the gun show. Based on the foregoing, your Affiant believes CEMAN may have had other individuals sell the firearms he

brought to the gun show on his behalf.

23. On December 5, 2024, your Affiant conducted surveillance of CEMAN at the PREMISES (i.e., N2607 County Road Q, Markesan, WI 53946). At approximately 9:27 a.m., your Affiant observed CEMAN, wearing a bright green and black jacket, exit the front door of the PREMISES, walk around its front porch area, and then reenter the PREMISES. Shortly thereafter, your Affiant observed the VEHICLE, previously identified as belonging to CEMAN, drive out of the attached garage. Your affiant observed CEMAN, who was still wearing the bright green and black jacket, driving the VEHICLE as it exited the PREMISES's driveway onto Highway Q.

24. Based on training and experience, your Affiant is familiar with certain behaviors and characteristics routinely associated with individuals involved in firearms trafficking. For instance, your Affiant knows that firearms traffickers often use electronic equipment, wireless and land line telephones, and pager to conduct firearms trafficking operations. Your Affiant knows that firearms traffickers often put their telephones in nominee names to distance themselves from telephones that are used to facilitate firearms trafficking. Your Affiant knows that firearms traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control (e.g., their automobiles), firearms, ammunition, and documents pertaining to such items. Regarding documents commonly under the dominion and control of firearms traffickers, such as records concerning firearms transactions (e.g., receipts indicating transfer of ownership, firearm purchase paperwork [e.g. ATF Form 4473, a Wisconsin DOJ Handgun Transfer form], photographs, financial records), such records can be stored in many different forms, including paper records and electronically (e.g. on cellular devices and computer hard drives).

25. Your Affiant believes that by obtaining the requested items and documents (whether in physical or electronic form), investigators will be able to obtain evidence regarding

CEMAN's alleged violations of 18 U.S.C. §§ 922(a)(1) (dealing firearms without a license) and 18 U.S.C. §§ 933 (firearms trafficking).

### **ELECTRONIC DEVICE BACKGROUND**

26. Your Affiant has participated in several firearms trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

27. Based on my training and experience, regarding electronic devices, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on CEMAN, the PREMISES or in the VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium is found on CEMAN, the PREMISES or in the VEHICLE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on CEMAN, the PREMISES or in the VEHICLE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium

that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks



and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate

conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it

requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium,

that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the

ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or

has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.
- h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would

permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

34. Because others may share the PREMISES as a residence, or the VEHICLE, it is possible that the PREMISES and the VEHICLE will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **CONCLUSION**

I submit that this affidavit provides probable cause for a warrant to search the property described in Attachment A to seize the items described in Attachment B.



## ATTACHMENT A

### *Property/person to be searched*

1. The PREMISES located at N2607 County Road Q, Markesan, Wisconsin 53946, further described as single-family, two-story home with an attached two car garage, brown siding and brown shingles. The premises sits on approximately 41 acres of property, which also includes four outbuildings/sheds/storage buildings. One of the buildings is a wooden outbuilding. There is a large wooden barn and a large storage building with light gray siding and black shingles. Lastly, there is a large blue shed located on the property.



The PREMISES (residence)



The PREMISES (outbuilding)



The PREMISES (barn and storage building)



The PREMISES (barn, building, and shed)

2. CEMAN's VEHICLE, further described as a red 2011 Chevrolet Silverado, bearing Wisconsin Registration GJ6336, and having VIN 3GCPKSE34BG339494.
3. The person of Michael G. CEMAN (Male/White, DOB 07/01/1957).

## **ATTACHMENT B**

### *Property to be seized*

Evidence of violations of 18 U.S.C. §§ 922(a)(1) (dealing firearms without a license) and 18 U.S.C. §§ 933 (firearms trafficking) involving, Michael G. CEMAN (Male/White, DOB 07/01/1957), including the following relating to such offenses:

- a. Records showing CEMAN's identity and any persons who supplied and acquired firearms to/from CEMAN;
- b. Records of purchases, transfers, and sales of firearms;
- c. Records of CEMAN's schedule, travel, and location at relevant times;
- d. CEMAN's financial records, such as bank accounts/statements, checks, and credit card bills;
- e. Relevant pictures, videos, IP addresses, contact information, and contact lists;
- f. Text messages, social media messages and content, SMS messages, iMessages, and related data regarding the sale and trade of firearms and controlled substances;
- g. E-mail content and addresses relating to the sale and trade of firearms and controlled substances;
- h. Computers or storage media used as a means to commit or facilitate the violations described above, including mobile/cellular phones;

For any computer or storage media that is authorized to be seized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise covered by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including

firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

The terms “records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.